DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AFI 31-401

AIA
Supplement 1

14 July 1997

Security

MANAGING THE INFORMATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AIA WWW site at: http://pdo.pdc.aia.af.mil/library/pubs.

OPR: HQ AIA/SOCD (MSgt J. B. Case III)
Supersedes AFI 31-401 AIA Sup 1, 12 January 1996.

Certified by: HQ AIA/SO (Mr. Robert P. Egger)
Pages: 5
Distribution: F; X: AF/SPI/SPIB (1 each); AUL/LSE (1); TSS/ADW (2); HQ AIA/SO (5)

AFI 31-401, 22 July 1994, implements AFPD 31-4, Information Security, 1 November 1995, and is supplemented as follows:

This supplement implements the Information Security Program requirements for the Air Intelligence Agency (AIA). This supplement applies to all AIA activities and administratively supported activities worldwide. This supplement also applies to AIA-gained IMA (individual mobilization augmentees) and AIA-gained ANG (Air National Guard) and AFRES (Air Force Reserves) units.

SUMMARY OF REVISIONS

The AIA Commander (AIA/CC) no longer designates original classification authorities (OCAs). The OCA list for AIA and AIA administratively supported units is revised. Identifies circumstances requiring the mandatory use of secure facsimile machines are identified. Outlines specific procedures for turn-in of equipment and introduces AIA Form 255, Security Inspection of Equipment .

1.1.8. (Added) AIA Special Security Officer. The AIA Chief of Security (HQ AIA/SO) is the AIA Special Security Officer.

1.1.9. (Added) Special Security Contact Officer (SSCO). The wing, groups, centers, and units with a sensitive compartmented information facility (SCIF) appoint the information security program manager (ISPM) as the SSCO to perform sensitive compartmented information (SCI) management duties. Each HQ AIA directorate and special staff office and other AIA activities will appoint their additional duty security manager as the SSCO.

1.2.4. Requests for OCA are routed through the appropriate command channels to the Information Security Division (HQ AIA/SOC).

1.2.5. OCAs at AIA and AIA administratively supported activities' OCAs are listed in Attachment 1.

2.2. At each level of command, the ISPM monitors classification challenge requests and sends classification challenges of non-Air Force originated information to HQ AIA/SOC.

2.4.3.3. (Added) Submit an information copy of damage assessment to HQ AIA/SOC.

4.2.3. All magnetic media used on computer systems must be labeled with the highest classification level of the information on the system.

6.8.4.3. AIA/CC or his or her designee closes formal investigations for AIA.

8.7.4.1. (Added) The DD Form 2501 or a courier authorization letter, as directed by governing directives, is required when transporting classified material into or out of AIA-controlled or restricted areas.

8.7.4.2. (Added) The issuing organization controls DD Form 2501 before the form is issued. The organization is not responsible for maintaining the card when the cardholder is not performing courier duties. The cardholders are responsible for these duties.

8.7.4.3. (Added) Couriers receive approval from wing, group, or center commanders to take any classified collateral material aboard commercial aircraft outside the United States. HQ AIA/SOP is the approval authority for HQ AIA personnel and offices.

8.7.5.2.1. (Added) Security managers periodically brief and maintain briefing statements in local files until members are no longer assigned or performing courier duties.

8.7.5.4. (Added) Secure facsimile transmissions will be required in certain situations.

8.7.5.4.1. Transmit all transmissions to and from US Defense AttachÈ Offices via secure facsimile.

8.7.5.4.2. For overseas to overseas locations, send all transmissions which are not purely administrative via secure facsimile.

9.1. Protect and destroy all administrative paper products such as working papers, notes, etcetera, located in open storage areas, SCI-working areas, or facilities the same as classified waste.

9.1.2. Equipment approved for the destruction of SCI material is also authorized for the destruction of all classified material.

9.1.3.1. (Added) Return all Top Secret material to the unit TSCO (Top Secret Control Officer) for destruction.

9.1.7. (Added) To seal bags, use staples or tape across the top of DDS (Document Destruction System) bags containing classified waste. Mark according to procedures outlined in DoD S-5105.21-M-1, chapter 3, paragraph T.5.

9.2. (Added) Proceedures for Destroying Classified Material. Equipment custodians will ensure all equipment (including furniture) which has processed or held classified information is properly disposed of when no longer needed.

9.2.1. Clear all computer equipment of all classified data by wiping hard drives and ensuring all floppy diskettes and labels are removed. Ensure local directives are provided by the local computer security representatives.

9.2.2. Carefully inspect furniture, lockers, security containers, and equipment racks for classified information. All personnel turning in equipment will contact their security manager or SSCO. The AIA Form 255 or other locally designed form, must be used to process all turn-ins. Attach one signed copy of the form prominently to the equipment for inspection by pick-up personnel.

9.2.3. The Equipment Custodian will facilitate the disposition of all laser printer cartridges. Establish local policies that as a minimum require five pages of random text to be run through. Units should make every effort to be active members of the installation recycling program. Overseas, more stringent measures apply.

10.1. Security managers develop security education material to ensure newly assigned personnel are briefed on DoD, Air Force, AIA, and local security requirements.

10.2.1. Security managers support supervisors by ensuring personnel receive continual education and training. Accomplish recurring training, an on-going process, quarterly.

10.2.2. (Added) Security managers or SSCOs will provide and document annual training on secure fax procedures. (This may be an inspectable item in unit effectiveness inspections and in staff assistance visits.)

10.3.1. Security managers or supporting SSCOs will provide foreign travel briefings to all personnel prior to travel but, as a minimum, annually. Travelers must make briefing arrangements as soon as travel requirements become known. USAFINTEL 201-1 outlines procedures for official and unofficial travel of SCI-indoctrinated individuals.

10.6. (Added) Security Training, Education, and Motivation (STEM) Program. Each AIA unit and supported activity will establish a consolidated STEM program to ensure security education requirements are met. Unit ISPMs manage the unit STEM program. Unit commanders or designated representatives should chair all STEM meetings. Program membership consists of representatives from the following security disciplines:

Automated Information Systems and Network Security.

Industrial security, information security.

EMSEC (emission security).

SCI Management.

Physical Security.

Operations Security.

Personnel Security.

10.6.1. AIA units having less than 30 personnel do not need to conduct STEM meetings. Units in this category, on a quarterly basis, distribute security education materials and address any problem areas that the unit experiences in the previous quarter.

10.6.2. The 67th Support Squadron Security Office (67 SPTS/SO) oversees the STEM program for HQ AIA directorates, collocated units, and the 68th Intelligence Squadron.

12.2.1. (Added) The Directorate of Operations, Operations Support, Policy Branch (HQ AIA/DOMP) assigns, controls, and monitors nicknames used by elements of AIA and administratively supported units.

12.2.2. (Added) Units are responsible for notifying HQ AIA/DOMP when a nickname is required, transferred to another office, or when no longer required. Use AF Form 608, Nickname Assignment/Change/Cancellation Request Notification.

12.2.3. (Added) Each group, center, and wing will appoint a local nickname monitor to assist in semiannual reviews of that unit's assigned nicknames.

13.2. The senior security force member assigned to an AIA unit is the ISPM. The unit commander will appoint an individual as ISPM where no security force member is assigned.

13.4. A DIA (Defense Intelligence Agency) SCI management inspection during a group level or higher information security staff assistance visit may replace one of the semiannual self-inspections.

13.5.2. Provide MIS (Management Information System) reports to HQ AIA/SOC no later than 25 January and 25 July in support of the requirements outlined in AFPD 31-4, Attachment 1, paragraph A1.2.

13.6. (Added) Forms Prescribed: AIA Form 255.

Attachment 1

AIR INTELLIGENCE AGENCY ORIGINAL CLASSIFICATION AUTHORITY LIST

A1.1. The following AIA and administratively supported units' officials are designated as OCA for the level listed:

A1.1.1. TOP SECRET:

AIA Commander (AIA/CC).

AIA Vice Commander (AIA/CV).

Commander, National Air Intelligence Center (NAIC/CC).

Commander, Air Force Technical Applications Center (AFTAC/CC).

A1.1.2. SECRET:

Technical Director (AIA/CA).

Director of Operations (HQ AIA/DO).

Director of Plans and Requirements (HQ AIA/XR).

Commander, Air Force Information Warfare Center (AFIWC/CC).

NAIC Director, Technical Assistance (NAIC/TA).

Commander, 67th Intelligence Wing (67 IW/CC).

Commander, 26th Intelligence Group (26 IG/CC).

Commander, 692d Intelligence Group (692 IG/CC).

Commander, 694th Intelligence Group (694 IG/CC).

ROBERT P. EGGER
Chief of Security